Identity Theft Response Checklist

1. Place a "Fraud Alert" on your credit report

- Regardless of whether or not thieves have already misused your personal information, the most important thing that you can do is minimize the damage done to your credit report.
- By placing a fraud alert on your credit report, you can stop any further damage or even prevent problems in the first place.
- The fraud alert tells creditors to contact you directly before opening any new accounts or making any changes to your existing accounts.
- Because the three credit bureaus are required by law to contact each other and share information about fraud alerts, you only need to contact one of the three companies to place an alert on all your accounts.
- An initial fraud alert stays on your credit report for 90 days and entitles you to a free copy of your credit report.
- If you are certain that identity thieves have used or attempted to use your personal information, you can place an extended fraud alert on your credit report. The extended alert remains in effect for seven years and entitles you to two free credit reports within twelve months from each of the three nationwide consumer reporting companies.
- Also, if you file an extended fraud alert the consumer reporting companies will remove your name from marketing lists for pre-screened credit offers for five years, unless you ask them to put your name back on the list before then.
- Once you have placed the fraud alert in your file, please take advantage of your right to free copies of your credit report in order to make completely sure that you know the full extent of the damage to your credit report.
- Review your reports for suspicious activity, like inquiries from companies you did not contact, accounts you did not open, and debts on your accounts that you cannot explain.
- Check to be sure that your personal information - like your SSN, address, name or initials, and employers - is correct.

- Also, watch for other signs that your information is being misused. A missing bill or financial statement could mean an identity thief has taken over your account and changed your billing address to cover his tracks. Other signs include receiving credit cards that you didn't apply for; being denied credit or being offered less favorable credit terms, like a high interest rate, for no apparent reason; and, getting calls or letters from debt collectors or businesses about merchandise or services you did not buy.

2. Contact the relevant account providers or agency

- Whether an unauthorized account has been opened in your name or you have become aware of unauthorized activity on an existing account, it is critical to contact the entity with which the account exists immediately in order to limit the harm identity thieves can cause.
- Be sure to close the accounts that you know or believe have been tampered with or opened fraudulently.
- If the stolen information includes your driver's license or other government-issued identification, contact the agencies that issued the documents and follow their procedures to cancel a document and get a replacement.
- Ask the agency to "flag" your file to keep anyone else from getting a license or another identification document in your name.
- Ideally, you should write down the emergency contact phone numbers printed on the reverse of all credit and debit cards, as well as copy the emergency customer service numbers for all your utilities, including your cellular and home telephone providers, as printed on your most recent bill.
- REMEMBER, IDENTITY THEFT CAN OCCUR ANYWHERE. IF YOU ARE PLANNING A TRIP OUT OF THE COUNTRY, BE SURE TO CARRY WITH YOU A COPY OF THE INTERNATIONAL EMERGENCY NUMBERS FOR YOUR CREDIT AND DEBIT CARDS.
- If the theft involved stolen checks, contact the major check verification companies.
- Ask that retailers who use their databases not accept the checks on your closed account.
- To find out if the identity thief has passed bad checks in your name, call SCAN at 1-800-262-7771.
- If you are disputing unauthorized account usage or unauthorized new accounts, remember that you must prove to each company, where an account was opened or used in your name, that you did not create the debt.
- You can download an ID Theft Affidavit to assist you in making certain you do not become responsible for debts incurred by an identity thief: http://www.ftc.gov/bcp/edu/resources/forms/affidavit.pdf

- Most companies accept the Affidavit, but some require more or different information so contact the organization with which you are dealing before submitting the document.

3. File a report with your local police or the police in the community where the identity theft took place

- Most credit card issuers and utilities require proof of theft in order to begin the remediation process.
- Filing a report with your local police is crucial.
- If, however, the local police tell you that identity theft is not a crime in their jurisdiction, ask to file a Miscellaneous Incident Report in order to have a record of the theft.
- If they simply will not take a report, see contact your local Sheriff's Office of the Pennsylvania State Police.
- Regardless of what entity ultimately takes your complaint, be sure to get a copy of the report or, at the very least, the number of the report, to submit to your creditors and other organizations that may require it.

4. File a complaint with the Pennsylvania Attorney General's Bureau of Consumer Protection and the Federal Trade Commission

- While criminal complaints will help to get your life back on track, reporting identity theft to the appropriate government agencies is necessary to ensure that the full scope of law enforcement is brought to bear against thieves.
- Both the Attorney General and the Federal Trade Commission (FTC) maintain databases of identity theft cases, and will prosecute identity thieves to the fullest extent of both the criminal and civil law.
- The Attorney General may also be able to gain some restitution for you, the victim.
- Filing a complaint also helps us learn more about identity theft and the problems victims are having so that we can better assist the people of the Commonwealth.
- The Attorney General's Consumer Complaint Form can be downloaded using the following link: http://www.attorneygeneral.gov/uploadedFiles/Complaints/BCP_Complaint_Form.pdf
- Use the following link to file a complaint with the FTC: http://www.ftc.gov/bcp/edu/microsites/idtheft/index.html

5. Continue to review your financial account statements

- Identity thieves may not strike immediately so it is critical to remain vigilant with respect to your personal information.

- Monitor your credit reports every few months in the first year of the theft, and once a year thereafter.
- Follow up with utilities and credit card issuers to be sure that no unauthorized activity has occurred on your accounts or under your name.

Use the following link to access contact information for credit reporting agencies, major financial institutions, government agencies and other organizations:
http://www.attorneygeneral.gov/uploadedFiles/Consumers/ID_Theft/full_contact_list.pdf